NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

STRATEGY FOR LOCAL LAW ENFORCEMENT AGENCIES TO IMPROVE COLLECTION, ANALYSIS, AND DISSEMINATION OF TERRORIST INFORMATION

by

Christopher Cleary

March 2006

Thesis Advisor:	Robert Simeral
Second Reader:	Christopher Bellavita

Approved for public release: distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Strategy for Local Law Enforcement Agencies to Improve Collection, Analysis and Dissemination of Terrorist Information			**5. FUNDING NUMBERS**
6. AUTHOR(S) Christopher Cleary			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Nassau County Police Department 1490 Franklin Ave, Mineola NY 11501			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release: distribution is unlimited			**12b. DISTRIBUTION CODE**

13. ABSTRACT (maximum 200 words)

Local law enforcement agencies play a significant role in domestic counter-terrorism and homeland security. The intelligence function of law enforcement agencies enhances their ability to detect criminal activity related to terror groups, as well as the ability to prevent, or respond to a terrorist attack.

This research project identifies policies and procedures that could be implemented by local law enforcement agencies to enhance cooperation and collaboration with other public sector agencies, private sector security providers, and the general public. The policies and procedures are based on intelligence-led policing and public-private partnerships, and will generate the ability to increase the flow of information disseminated from, and collected by, law enforcement intelligence entities. The resulting intelligence developed by law enforcement intelligence can be pushed up to the state and national level to improve the nation's ability to detect potential terrorist activity, protect citizens, and safeguard critical infrastructure.

14. SUBJECT TERMS Intelligence Sharing - Information Sharing - Local Law Enforcement			**15. NUMBER OF PAGES** 73
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release: distribution is unlimited

STRATEGY FOR LOCAL LAW ENFORCEMENT AGENCIES TO IMPROVE COLLECTION, ANALYSIS, AND DISSEMINATION OF TERRORIST INFORMATION

Christopher J. Cleary
Deputy Inspector, Nassau County Police Department
B.S., New York Institute of Technology, 2000

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
March 2006**

Author: Christopher J. Cleary

Approved by: Robert Simeral
Thesis Advisor

Christopher Bellavita
Second Reader

Dr. Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Local law enforcement agencies play a significant role in domestic counter-terrorism and homeland security. The intelligence function of law enforcement agencies enhances their ability to detect criminal activity related to terror groups, as well as the ability to prevent, or respond to a terrorist attack.

This research project identifies policies and procedures that could be implemented by local law enforcement agencies to enhance cooperation and collaboration with other public sector agencies, private sector security providers, and the general public. The policies and procedures are based on intelligence-led policing, and public-private partnerships and will generate the ability to increase the flow of information disseminated from, and collected by law enforcement intelligence entities. The resulting intelligence developed by law enforcement intelligence can be pushed up to the state and national level to improve the nation's ability to detect potential terrorist activity, protect citizens, and safeguard critical infrastructure.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

This thesis was completed with the help, support and guidance of many people. I would like to thank Commissioner James H. Lawrence of the Nassau County Police Department for recognizing the importance of the CHDS program and for providing me the opportunity to participate. I would also like to thank Chief of Department Raymond Crawford (Ret.) and current Chief of Department Anthony Rocco for their continued encouragement and for allowing me to complete this program while working as a member of their staff.

Thank you to my advisors Robert Simeral and Chris Bellavita for all their invaluable help in the completion of this thesis and to Joan Charles for her help in editing.

I am grateful to the faculty and administrative staff at the Center for Homeland Defense and Security. They are a remarkable group of people who provide their students with friendship and an unparalleled learning environment.

I must also recognize the women and men of cohort 0403 and 0404. During the course of this program I learned a great deal from each of them, and I am truly proud to be a member of their group.

My participation in this program would not have been possible without the love and support of my wife Tracy and our children Shane, Ryan, Brendan and Kerrin. I thank you all for your patience and your encouragement.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

In the months following the terror attacks of September 11, 2001, members of the law enforcement community recognized the need for comprehensive intelligence in order to comply with the objectives outlined in the National Strategy for Homeland Security.[1] Law enforcement executives throughout the country have responded to meet this need by increasing manpower and equipment resources in their criminal intelligence units. In spite of this new commitment to intelligence, most agencies have yet to fully develop adequate policies and procedures to make the intelligence more actionable and relevant to the goal of enhancing homeland security. In order for local law enforcement agencies to contribute to a national counter-terror intelligence network, there is a need to determine the most effective methods for information gathering and analysis, and for the dissemination of intelligence that could be used to detect and disrupt terrorist activity being conducted within the continental United States.

It has become widely accepted that law enforcement agencies need to participate in a collaborative counter-terrorism network. The 9/11 Commission report stressed the need for a unity of effort in sharing information, and the importance of intelligence analysis that could draw upon all relevant sources of information.[2] Prior to 2001, intelligence units in local law enforcement agencies were focused on collecting information related to domestic criminal activity, such as organized crime and illegal narcotics sales. Unfortunately, most agencies simply increased their pre-9/11 activities, and failed to recognize the need to develop a new intelligence strategy. In spite of the obvious need to share information, many agencies have also failed to institute policies or adopt procedures that encourage the prompt dissemination of intelligence to law enforcement and non-law enforcement government agencies, as well as to private security agencies that protect vital infrastructure.

---

1 The *National Strategy for Homeland Security* identified three strategic objectives: preventing terrorist attacks within the United States; reducing America's vulnerability to terrorism, and minimizing the damage and recovery from attacks that do occur.

2 Thomas H Kean, Lee H Hamilton, The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States (New York: W.W. Norton, 2004), 417.

There is also a need for agencies to recognize that the information collection process must involve all sworn members, and not be limited to only those investigators assigned to counter-terrorism cases. Modern terror groups are employing criminal enterprises such as larceny, drug trafficking, forgery and identity theft in order to further their goals, or finance their missions. Uniformed patrol officers are usually the first to become aware of suspicious activity related to these crimes, unfortunately the information does not often reach the local intelligence unit. By integrating intelligence-led policing policies, departments can increase the amount of information that is collected, and actually produce terrorism intelligence instead of merely utilizing intelligence passed down from State and Federal sources.

In order to develop a robust domestic intelligence network that will be truly useful in providing protection from terror activity within our borders, agencies must adopt strategies and standards of intelligence and information management. The intelligence management model should adopt a structure for the integration of agency-wide intelligence, file protocols, as well as security clearances and training requirements for analysts.

A robust domestic law enforcement intelligence network is essential for providing protection from terror activity within our borders. As the network grows with the addition of more participating agencies, the adoption of strategies for improving intelligence and information management will help to form a more unified system. This unity will aid in the development of new methods and strategies that can be employed to detect, and / or deter terrorist activity, protect potential terror targets, and to hasten recovery efforts if an attack should occur. Once these counter terrorism strategies are identified, agencies will be able to focus their assets to develop actionable intelligence in support of the strategies.

B. RESEARCH QUESTION

This research project will attempt to identify the policies and procedures that should be implemented in order to fulfill the current and future intelligence needs of local police agencies, in order to enhance the nation’s ability to detect potential terrorist activity, protect citizens, and safeguard critical infrastructure.

C. SPECIFIC RESEARCH OBJECTIVE

The objective of my research is twofold; I will identify best-practices that are currently in use by State, and local intelligence units, and I will seek to identify cost-effective strategies for the implementation of a new intelligence paradigm in order to provide guidance to law enforcement executives. The new paradigm will identify recommendations for improving information collection, training standards for intelligence analysts, strategies for inter-agency cooperation, as well as proper formats for intelligence dissemination. This research will focus on developing a strategy to incorporate the intelligence function throughout the various disciplines that are inherent in modern law enforcement agencies, and to identify readily available sources of information that have gone untapped by law enforcement intelligence analysts.

D. SIGNIFICANCE OF RESEARCH

According to a recent study conducted in cooperation with the International Association of Chiefs of Police (IACP) by the Justice Department's Community Oriented Policing Services (COPS) during the year 2000 there were 17,784 state an d local law enforcement agencies in the United States, employing 708,000 full-time sworn officers. By contrast, there were only 88,500 federal law enforcement officers.[3] Employing the vast resource of State and local agencies would surely enhance the effort to reduce the threat and impact of terrorism in the United States. The development and adoption of standards in the field of intelligence will create a broad-based network response to terrorism by combining the resources of all law enforcement agencies.

E. REVIEW OF RELEVANT LITERATURE

The focus of this research is to identify a viable structure for the further integration of the intelligence function into current law enforcement practices and methods. In my research to date, I have found that leading experts have recognized the need to improve the intelligence function at the local level and have proposed many ideas that might help to improve organizational structure as well as the quality of the deliverable intelligence product.

[3] IACP, COPS. Private Security/Public Policing Partnerships *(Washington D.C. 2004),* 1 http://www.cops.usdoj.gov/mime/open.pdf?Item=1355. Last accessed 12/08/05.

In his Guide for State, Local, and Tribal Law Enforcement Agencies, Dr. David L. Carter[4] advocates the need for structure and standardization regardless of the size of the Agency or the availability of manpower. He stated, "common standards, policies, and practices will help expedite intelligence sharing while at the same time protect the privacy of citizens and preserving hard-won community policing relationships." These community policing relationships will be useful in the development of local criminal intelligence because the COP officers have "immediate and unfettered access to local, neighborhood information as it develops." Carter recognizes that the relationships that have been developed over the past decades should not be abandoned, but should be a cornerstone of what he describes as a shift into "intelligence-led policing"(ILP).[5]

A 2005 study sponsored by the Police Executive Research Forum reinforces the arguments made by Carter. The study, Protecting the Community from Terrorism, volume 4, advocates the need for an organization-wide commitment to change in order to fully incorporate ILP. The PERF study calls for the development of "cadres of intelligence and analytic experts who are professionally trained and educated" in order to develop a collaborative national network.[6] An analyst's training should include a national and local perspective to avoid "passivity" in which analyst simply respond to requests for information, without performing any substantive analysis.

To address the need for structure, an Intelligence Working Group sponsored by the International Association of Chiefs of Police (IACP) produced a National Criminal Intelligence Sharing Plan outlining recommendations for better methods of sharing critical data among all law enforcement agencies.[7]

In addition to calling for unity of effort in intelligence sharing among law enforcement agencies, the 9/11 Commission also spoke about the over-classification of

[4] David L. Carter, *Guide for State, Local, and Tribal Law Enforcement Agencies* (East Lansing: Michigan State University, 2004), 2-4. http://www.cops.usdoj.gov/Default.asp?Item=1404. Last accessed 10/15/05.

[5] Carter, *Guide*, 40.

[6] Loyka et al., *Protecting the Community from Terrorism, volume 4* (Washington D.C. Police Executive Research Forum, 2005) 29 http://policeforum.mn-8.net/default.asp?link=%2Fdocs%2Fdocapp%2Easpx%3F%5Fcommand%3Ddetail%26%5Fappid%3D5%26id%3D41645%26%5FclientInfo%3D%253cclientInfo%253e%253cfid%253e%2D1%253c%252ffid%253e%253c%252fclientInfo%253. Last accessed 09/21/05.

[7] Department of Homeland Security, *National Criminal Intelligence Sharing Plan*.

information and how there is no punishment for failing to share information. They recognize the importance of sensitive material, but stress the need to create a "trusted information network" which would operate on a "need to share" basis.[8] The nation's most critical infrastructure locations are often controlled by private security agencies that do not have access to counter-terrorism intelligence. It is necessary for agencies to create information sharing networks, which will facilitate the transfer of information between law enforcement and the private sector.

The IACP, COPS study on Private Security/Public Policing Partnerships claimed that there are 90,000 private security organizations employing roughly 2 million security Officers in the United States. The study suggested, however, that only five to ten percent of law enforcement chief executives participate in any collaborative partnerships with private security. The study recommends that leaders of the major law enforcement and private security organizations should endorse the implementation of sustainable public–private partnerships in order to address terrorism, public disorder, and crime.[9] In order to avoid the release of sensitive information, Dr Carter provides general rules for the release of information. He advocates that intelligence analysts prepare two versions of an intelligence product if it becomes necessary to release information outside of law enforcement, an unclassified public version, and a "Law Enforcement Sensitive" version. The Law Enforcement Sensitive version would provide more detailed information about suspects. If there is a credible threat to a civilian target it may become necessary that both strategic intelligence and tactical intelligence be disseminated as quickly as possible.[10]

F. HYPOTHESIS

Local law enforcement agencies play a significant role in counter-terrorism and homeland security. The intelligence function of these agencies enhances their ability to detect criminal activity related to terror groups, as well as the ability to prevent, or respond to a terrorist attack. Since many existing intelligence policies and procedures are

8 See note 2 above.

9 IACP, COPS. 2004. Private Security/Public Policing Partnerships. 2 http://www.cops.usdoj.gov/mime/open.pdf?Item=1355. Last accessed 12/08/05.

10 Carter, *Guide*, 83.

inadequate for the homeland security mission, there is a need to provide guidance for improving the intelligence structure within law enforcement agencies in order to make the agency better able to fulfill its expected role in the homeland security effort.

G. METHODOLOGY AND SOURCES

(a) Literature review of current information regarding the most useful policies to implement to integrate the intelligence function throughout a local law enforcement agency, identify training standards for analysts, and improve the quality of the intelligence end-product.

(b) Case study will examine successful strategies that are currently producing verifiable successes. Identification of best practices could be used to guide local law enforcement decision makers to allocate their resources into areas that will provide the best chance of success in increasing preparedness, and in identifying criminal or suspicious activity that may be a precursor to a terrorist event.

The cases that I will compare include, but are not limited to:

- The New York Office of Homeland Security's Operation Safeguard as an example of Intelligence-Led Policing techniques used as the basis of an anti-terrorism program.
- The Los Angeles Terrorism Early Warning Group as an example of how the resources of non-law enforcement public agencies can be integrated with those of law enforcement to enhance the intelligence network.
- The Nassau County Police Department Security Police Information Network as a model for incorporating the resources of private security agencies into the law enforcement intelligence network.

II. THE LAW ENFORCEMENT INTELLIGENCE NETWORK

The law enforcement intelligence network is essential to the responsibility of providing protection from terrorism in the United States. Not all law enforcement agencies will have the resources to develop a full intelligence function, but all can benefit from a better understanding the intelligence process, because the basic steps in the process take place either formally or informally in every law enforcement agency. Understanding the principles of the intelligence process, the common terminology, and the most effective methods for consuming the intelligence products that are disseminated by network participants will enhance an agencies ability to reduce crime and provide homeland security.

The initial homeland security efforts in the United States have focused primarily on developing strategies, conducting training, and obtaining equipment that will be used in response to a successful terror attack. Since a great deal of attention was given to the heroism, leadership, response and recovery to the 9/11 terror attacks, many decision makers were focused on repeating those successes. Federal, State and local law enforcement agencies have spent vast sums of money to purchase personal protective equipment, response vehicles, and search and rescue equipment, all of which could be used after a successful terror attack. The majority of anti-terrorism training and exercises have focused on response to Chemical, Biological, Radiological, Nuclear, Explosive (CBRNE), and other mass casualty events. While these efforts have been worthwhile, expanding the focus to include counter-terrorism activities such as the detection of terrorists, and the prevention of attacks is the best way for police agencies to achieve the ultimate goal of protecting citizens from an attack.

A. WHAT IS INTELLIGENCE?

Attaining the most benefit from the intelligence products requires some understanding of terminology and processes. The term “intelligence” has different meanings depending on its use. For example “intelligence” is often used to describe the “The Intelligence Community”, the Federal and Military agencies involved in national security. It is also used to describe the process of collecting, exploiting, analyzing, and

disseminating data to support strategic plans. “Intelligence” is also used in referring to the unit within an agency that performs these functions. The most accurate meaning relative to this discussion is that intelligence is the product that is produced when trained analysts exploit, evaluate, and focus information so that it supports a strategic need of the agency. Law enforcement agencies have access to a vast amount of information from an endless list of sources. The information is not intelligence until it is recognized, analyzed, and put into a format that supports the needs of the agency.

In this paper the term “intelligence” will be used to describe the finished product of the intelligence process. All other references will be noted as the “intelligence function,” the “Intelligence Unit,” or the “Intelligence Community.”

B. THE INTELLIGENCE PROCESS

The National Criminal Intelligence Sharing Plan[11] released in 2003 by the Bureau of Justice Assistance recognizes six steps in the law enforcement intelligence Process. The diagram shows that the process is not linear with clear beginning and ending points. The process is circular in that the effectiveness of intelligence products are evaluated to see how effectively they met the agencies needs, then that evaluation is used as the basis for future planning decisions.

[11] U.S. Department of Justice, *Intelligence-Led Policing: The New Intelligence Architecture*. 6.

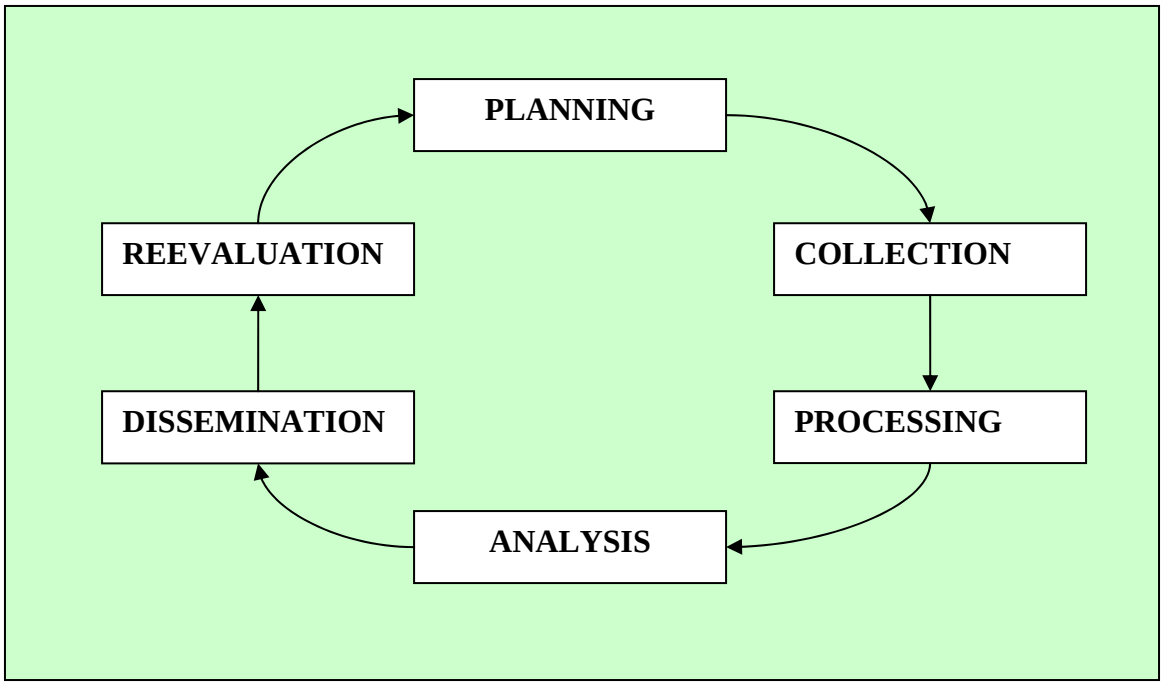

Figure 1. The Intelligence Process

1. Planning

Law enforcement agencies in the United States have varied missions, and therefore they have different intelligence needs. Many police departments conduct patrol, response, and investigation functions, while other agencies such as some Highway Patrols focus solely on enforcing laws, and promoting safety for vehicular and pedestrian traffic. Agencies like the Federal Bureau of Investigation do not conduct any patrol functions because all their efforts go into investigating criminal cases. Each agency adopts the most logical anti-terrorism, or counter-terrorism strategies, and therefore must determine the way in which intelligence can assist their particular efforts.

Just as specific intelligence requirements vary among agencies, requirements may also vary between units within an agency. A unit that investigates financial crimes may have different informational needs than a unit that investigates cybercrimes, or a unit that provides dignitary protection. Since most agencies have finite intelligence resources, a key component of the planning function for law enforcement agencies should be crime

analysis. Decision makers need to be governed by the analysis of crime patterns and trends when setting agency priorities or allocating intelligence resources.[12]

2. Collection

Law Enforcement agencies continuously collect information through processes such as observations, victim and witness reports, physical and electronic surveillance, confidential informants, electronic databases and news media accounts. As technology continues to improve, agencies are integrating more sources into the collection process. The Internet provides access to an overwhelming amount of information about people, locations, and events. Additional collection benefits may be realized through recruitment of younger analysts who have grown up with the Internet and the resulting information explosion that has occurred over the past fifteen years. The new analysts will be much more computer savvy, and more creative in their search for information[13].

In addition to the electronic and traditional methods for collecting information, this paper advocates expanding the collection process by employing intelligence-led policing techniques, and by utilizing the resources of the Public and Private sector to create new sources for information collection.

It is important to note that all decisions regarding the collection of information must be made with a careful regard for Federal, State, and local laws.

3. Processing

Processing is the function of separating relevant and factual data from the irrelevant and incorrect data, then cataloging the relevant data in a usable format.

In light of the large number of information sources, vetting information for accuracy and reliability can become time consuming. Agencies that use software to identify relevant files must examine and often investigate the information contained in the file to determine its validity. A database search may identify a case record that

---

[12] U.S. Department of Justice. *Law Enforcement Analytic Standards* (Washington D.C. 2004), 17 http://it.ojp.gov/documents/law_enforcement_analytic_standards.pdf. Last accessed 05/10/05.

[13] Treverton, Gregory F., The Next Step in Reshaping Intelligence, RAND Corporation (Santa Monica 2005), 21.

appears to have a relevance to terrorism, but the information should not be used as a basis for an intelligence report until the circumstances in the case record are verified through investigation. Police departments often create case reports based on witness accounts of suspicious activity. After investigation, many of these cases are closed because the seemingly suspicious activity is found to have a legitimate non-criminal purpose.

4. Analysis

Analysis is the process of assigning meaning to data. A law enforcement analyst reviews data and evaluates its value as it might relate to crime patterns, current investigations, or long-term strategic planning. The information is then converted to a format that can be used to support operational activities.

The analyst should indicate the facts that are know, as well as those that are incomplete or missing. Law enforcement intelligence products provide hypotheses about criminal offenders, crime patterns and trends, or other potential threats to the jurisdiction.

5. Dissemination

Dissemination is the process of getting actionable intelligence to those who have the need and the right to use it. This process requires continuous management to find the balance between sharing valuable information and withholding intelligence that might damage an investigation if released.

6. Reevaluation

Agency administrators must institute a procedure to assess the value and effectiveness of intelligence products. The assessment should involve the consumers of the information including the investigators and uniformed officers at the level of execution.

The continuous evaluation of the intelligence process should be the basis for future decisions made in the planning process.

C. THE CURRENT NETWORK

The law enforcement intelligence network is used primarily as a crime prevention tool. Traditional crime analysis involves sifting through crime reports within a jurisdiction looking for similarities that might indicate pattern crimes or recognizable trends. Indicators from crimes in local jurisdictions are now being shared among law enforcement agencies via the network. By comparing the indicators from neighboring jurisdictions, analysts are better able to recognize certain crime trends and patterns. Agencies use the information to develop strategies to arrest offenders and prevent future crimes. The communications link that exists among law enforcement intelligence units provides the ability for analysts to identify crime patterns and trends that exist beyond jurisdictional boundaries.

Inter-agency cooperation in a Federal, State, and local counter-terrorism intelligence network expands the nation's ability to detect criminal activity related to terror groups and the individuals and groups that provide their financial and logistic support. Prior to the 9/11 terror attacks there were legal and cultural obstacles for active integration of law enforcement intelligence with the Intelligence Community. The attacks demonstrated the ability of an adversary to operate both outside the U.S. and within our borders and created incentive for the melding of the resources of the Intelligence Community with those of law enforcement. Some of the restrictions that prevented Federal agencies from sharing information were removed by Executive Order issued in August of 2004.[14] Positive steps have been taken by the Federal Government and many State Governments to integrate intelligence functions, but a single link between intelligence units has yet to be created.

In the years since the attacks there have been constant complaints about a lack of specificity in the information provided to local police agencies. Many local officials have complained that their agencies are often asked to provide enhanced security at infrastructure locations based on incomplete information. In response, the FBI has developed a program in which local law enforcement agencies can designate a number of

[14] U.S. President, *Executive Order*. "Executive Order Strengthening the Sharing of Terrorism Information to Protect Americans" (27 August 2004) available online: http://www.whitehouse.gov/news/releases/2004/08/20040827-4.html. Last accessed 05/20/05.

"decision makers" who could apply for Secret security clearances. The Secret classification would allow local agencies to have access to information that could be used by the police, and also to provide the private agencies with a sanitized version to facilitate a more expansive security response. In addition to the Secret information, there are many new sources of official information available to local police agencies. Most police agencies have members who are able to cull open-source material from the constant stream of terrorism information classified as "Law Enforcement Sensitive" or "For Official Use Only" (FOUO).

Federal agencies control and regulate information that is classified as Confidential, Secret, and Top Secret.[15] Since State and local agencies do not have the ability to classify information as Confidential, Secret, or Top Secret, they rely on using a "Law Enforcement Sensitive" classification. This classification is intended to provide the ability to limit the distribution of sensitive information solely to other police agencies and agencies within the Intelligence Community (IC). Unfortunately this classification is not always respected. An inquiry using an internet search engine will provide links to posted documents that have the "Law Enforcement Sensitive' classification. There are at least two reasons that that this classification is ineffective: The first reason is that the classification is unofficial and there are no laws that prohibit the release beyond law enforcement members. The second reason is that it is often misused by law enforcement. A large amount of the intelligence distributed with a "Law Enforcement Sensitive" warning was collected from open sources such as news media.

With law enforcement agencies becoming active participants of a domestic intelligence network it is apparent that the Federal Government must recognize the necessity of protecting information that will be used to prosecute a criminal case and to protect the undercover investigators or confidential informants who may be endangered if

[15] U.S. President, *Executive Order*. "Classified National Security Information, Executive Order 13929" (25 March 2003) available online: http://www.fas.org/sgp/bush/eoamend.html. Last accessed 05/20/05.

the information is released. [16] The Government goes to great lengths to protect electronic collection sources, but fails to provide protection for the law enforcement professionals at the State and Local levels.

The National Counter-Terrorism Center (NCTC) was established by Executive Order in August of 2004 to act as the primary organization within the U.S. Government for the analysis and integration of foreign and domestic intelligence related to terrorism. In addition to some other responsibilities, the NCTC serves as a shared knowledge bank on known and suspected terrorists and international terror groups. Since there is no direct line of communication between the NCTC and local law enforcement agencies, terrorism intelligence products are transmitted through agencies including the FBI, and DHS.[17] The FBI currently issues numbered Counterterrorism Division Intelligence Bulletins. These documents are unclassified but usually contain the unofficial "For Official Use Only" or "Law Enforcement Sensitive" prohibition. To ensure distribution to all law enforcement agencies, the documents are sent to State Intelligence entities. The State entity then disseminates the bulletin to all law enforcement agencies within the state. Because these bulletins are released sporadically the numbering on the document makes it easy for local law enforcement agency to verify if any documents have not been received. DHS does not number their unclassified intelligence reports so it is difficult to insure that all products have been received.

The integration and coordination of these Federal, State, and local law enforcement agencies with agencies in the Intelligence Community will help close some intelligence gaps that currently exist, and reduce the terrorist's ability to operate in the United States. Until a single source for the transmission of data and intelligence is developed, analysts must visit several electronic sources in order to develop a comprehensive intelligence report, and more importantly, there is no method to insure that vital time sensitive intelligence is communicated to every agency that has a need for

---

[16] NYPD Deputy Inspector Michael O'Neil, Commanding Officer NYPD Counter Terrorism Division. Interviewed by author, Brooklyn N.Y. (1 September 2005).

[17] U.S. Department of Justice, "The FBI's Counterterrorism Program Since September 2001" (14 April 2004) 65. Available online: http://www.fbi.gov/publications/commission/9-11commissionrep.pdf. Last accessed 12/15/05.

the information. Local agencies must keep State and Federal officials aware of the need for a primary electronic intelligence network that can link the Federal, State and local partners.

Even without a single-source national link, the existing network enables participants to access a large pool of information and intelligence, and provides the ability to make local or proprietary data and intelligence available on a national level.

Several national and regional information-sharing portals are used by the various members of the network. The Regional Information Sharing System (RISS) has been providing criminal intelligence dissemination to LEA's since 1973. In 2003, RISS implemented the Anti-Terrorism Information Exchange (ATIX) to provide a conduit for the exchange of intelligence specific to homeland security. The FBI's Law Enforcement Online (LEO) is an online service that provides participants with FBI intelligence products, as well as space for special interest groups, chat rooms, and topical focus areas.

The Joint Regional Information Exchange System (JRIES) is one of the more effective methods for the electronic transmission of data and intelligence. Operating as a real-time secure virtual private network (VPN), all law enforcement participants that have been vetted and approved for access to the system can share data sources and collaborate on common investigations.[18]

The current structure of the law enforcement intelligence network does provide a limited amount of protection from any wide dissemination of sensitive information. Since the network does not utilize a central repository of information, the vast majority of information is kept at the local level. Information exchanged between network participants is limited to information on recognized crime patterns or threats, and inquiries about active criminal investigations. If any participating agency knowingly, or unknowingly, collects personal information in violation of applicable privacy laws, the damage will likely be contained, and hopefully identified, at that local level.

18 Carter, *Guide*, 133.

D. FUSION CENTERS

While many Federal, State, and local agencies have been producing quality intelligence products, there are issues that impede interagency intelligence sharing. Legal, procedural and cultural barriers add up to what the 9/11 Commission refers to as the "human or systemic resistance to sharing information".[19] The creation of Fusion Centers has become an effective method to overcome these sharing problems.

Simply stated, the Fusion concept is the co-location of intelligence resources and analysts from Federal, State, and local agencies into one intelligence center. The benefit to co-location enables analysts to call upon the information and collection abilities of all participating agencies and then integrate that data to produce a more complete intelligence product. Information gathered and held by the individual participating may only prove useful when it is related and analyzed with information held by other agencies.

The fusion model has evolved from existing law enforcement information-sharing networks.[20] The ability to assign manpower to a fusion center is usually limited to agencies that have a large workforce, and a large intelligence budget. The participation of Federal and State partners adds considerable resources and also enables the distribution of the intelligence product to local law enforcement agencies that lack their own intelligence resources.

---

[19] Kean, Hamilton, *The 9/11 Commission Report*, 416.

[20] NGA Center for Best Practices, Issue Brief: *Establishing State Intelligence Fusion Centers,* National Governor's Association (Washington D.C. July 2005) at: http://www.nga.org/Files/pdf/FusionCenterIB.pdf. Last accessed 11/20/05.

E. INTELLIGENCE IN NIMS

> The analysis and sharing of information and intelligence are important elements of ICS. In this context, intelligence includes not only national security or other types of classified information but also other operational information, such as risk assessments, medical intelligence (i.e., surveillance), weather information, geospatial data, structural designs, toxic contaminant levels, and utilities and public works data, that may come from a variety of different sources. Traditionally, information and intelligence functions are located in the Planning Section. However, in exceptional situations, the IC may need to assign the information and intelligence functions to other parts of the ICS organization. In any case, information and intelligence must be appropriately analyzed and shared with personnel, designated by the IC, who have proper clearance and a "need-to-know" to ensure that they support decision-making.
>
> – National Incident Management System

The National Incident Management System[21] provides a structure for a nationwide approach to the management of natural and manmade disasters, and is designed to facilitate coordination between Federal, State, and local entities involved in the response to, or the recovery from a critical incident. Given that the NIMS protocol dictates that incident management must include a process for gathering, sharing, and managing incident-related information and intelligence, the intelligence network will be the most effective system to fill this role.

The intelligence network has the ability to provide Incident Command with a better understanding of the nature of the incident, and its underlying causes. Incidents that have a criminal component, such as terror attacks, will rely upon the network to guide the investigation in identifying and arresting perpetrators. The intelligence capability enhances the ability to conduct accurate threat assessments, and then to disseminate the threat information to other jurisdictions so they can guard against potential coordinated attacks.

The active communication links that are being used by some law enforcement could be used to coordinate the response of civilian and military interagency support

21 Federal Emergency Management Agency, *The National Incident Management System.* http://www.nimsonline.com/ics_org_charts/intel_2.htm. Last accessed 09/15/05.

during crisis and consequence management situations. In the aftermath of the 9/11 attacks many Federal, State and local agencies sent representatives to the New York City Emergency Operations Center to coordinate the multi-agency rescue, recovery and consequence mitigation efforts at the World Trade Center site. When a need was identified, EOC personnel went directly to the various representatives to secure help from their respective agencies. The agency representative made contact with his / her agency to see if resources could be directed to the affected area. Electronic resources available in the intelligence network, such as the Area Security Operations Command and Control (ASOCC) system,[22] can improve this process because of its ability to create a "Virtual" Emergency Operations Centers, and to provide a secure system for transmittal of intelligence. Operations personnel can push resource requests via ASOCC directly to other agency headquarters creating improved inter-agency collaboration in support of both administrative functions and field operations. A real-time connection between ASOCC participants allows intelligence staff to monitor situations and maintain an understanding of critical events as they develop.[23] The ASOCC system enhances the Common Operating Picture and as a result a coordinated civilian and military inter-agency response to critical incidents.

F. CHAPTER SUMMARY

- The intelligence process takes place in every law enforcement agency, even those without a staff dedicated to providing intelligence analysis. Administrators should recognize the benefits of using intelligence in developing short and long term crime reduction and homeland security planning.
- The National Counter-Terrorism Center is the primary organization within the U.S. Government for the analysis and integration of foreign and domestic intelligence related to terrorism. Law enforcement agencies receive unclassified intelligence developed at the National Counter-Terrorism Center through intermediary agencies such as the FBI and DHS.

---

[22] The Area Security Operations Command and Control System (ASSOC) is a secure communications portal available to law enforcement agencies that is able to provide a direct communications link between Federal, DoD, State, and local agencies throughout the United States.

[23] U.S. Department of Justice, Area Security Operations Command and Control System: Evaluation Report (Washington D.C. April 2005) http://www.ncjrs.gov/pdffiles1/nij/grants/212187.pdf. Last accessed 12/05/05.

Local agencies should press the NCTC to improve the process by creating a single path for the flow of intelligence, and to make more actionable and relevant intelligence available.

- The FBI has instituted a program to provide Secret security clearances to decision makers in local law enforcement agencies. Local agencies should apply for the Secret classification and thereby access information that could be used to enhance local security plans and direct enforcement efforts.
- Without a single-source national intelligence link, the law enforcement intelligence network enables participants to access a large pool of information and intelligence, and provides the ability to push local and proprietary data and intelligence up to the regional and national level. Local Agencies such utilize data sources such as RISS, ATIX, LEO, and JRIES to access and exchange information and intelligence.
- Local agencies must push Federal officials to develop a primary electronic intelligence network that can link the Federal, State and local law enforcement partners. A single intelligence link with help to eliminate the gaps that exist between the NCTC and local agencies.
- The co-location of multi-agency intelligence resources in a Fusion Center enables analysts to call upon the information and collection abilities of all participating agencies and then integrate that data to produce a more complete intelligence product. Although many agencies lack the resources to assign staff to a Fusion Center, the participating Federal and State agencies usually disseminate the resulting intelligence products to all local agencies.
- NIMS has been adopted as the national model for critical incident management. Since NIMS protocol dictates that the incident command structure must include the ability to gather, share and manage incident-related intelligence, the existing law enforcement intelligence should be used to provide this function.

THIS PAGE INTENTIONALLY LEFT BLANK

III. INTELLIGENCE LED POLICING

Community Policing techniques have been accepted by law enforcement agencies throughout the country. Central among the primary tenants of Community Policing is the understanding that agencies must work together with the community to set policing priorities and to reduce crime. The community policing partnerships start when police administrators confer with community leaders but often the more profound collaboration develops when officers, at the level of operation, interact with private citizens. Positive interactions between the police and the public produce mutual understanding and common goals so that the police agency is able to adapt operations to meet the needs of the community more directly and precisely. Additionally, community collaborations help police agencies develop better environmental scanning and enhanced crime prevention.[24]

Another benefit the law enforcement agencies have derived from Community Policing is structured problem solving techniques. Problem-Oriented-Policing is a Community Policing method that uses the SARA (Scanning, Analysis, Response, and Assessment) model as a way to recognize and prioritize problems, determine the actual cause of problems, develop a method to eliminate the problem, and assess the effectiveness of the response.

When agencies use this method they stimulate officers' creativity and resourcefulness to eliminate the root causes of recurrent calls thereby decreasing crime, and increasing police morale and community satisfaction.[25]

International terror groups have demonstrated their ability to integrate themselves into our society, and to use creative methods to achieve their goals. In addition to international terrorist groups, domestic groups that advocate terrorism as a tactic to cause societal change are living and working in local communities. Maximizing the ability of the intelligence network to fight these groups must involve the entire law enforcement system. By utilizing resources beyond those traditionally used in law enforcement, and

---

[24] US Department of Justice, Office of Community Oriented Policing Services *What is Community Policing?* http://www.cops.usdoj.gov/?Item=36. Last accessed 01/14/06.

[25] U.S. Department of Justice, Office of Community Oriented Policing Services "The SARA Model" available from website: http://www.popcenter.org/about-SARA.htm. Last accessed 01/14/06.

integrating all available resources into an information sharing structure, local police departments can increase the amount of information that is collected. The information can then be used to produce home-grown terrorism intelligence which will be more relevant for local policing needs than the "all-purpose" intelligence passed down from State and Federal sources. The intelligence requirements of State and local agencies are slightly different than those of Federal law enforcement agencies. In addition to investigating and prosecuting criminal acts as Federals do, State and local LEA's also strive to prevent criminal activity, which requires an enhanced level of situational awareness.[26] It stands to reason that an enhanced level of local situational awareness would prove to be a powerful antiterrorist tool.

Since the advent of modern policing, patrol officers have honed the ability to detect suspicious behavior in order to disrupt criminal enterprise. With the introduction of terror activity in the U.S. these same skills could be adapted to include the recognition of terrorist activities that may pose a danger to a much larger percentage of the populace. Modifying the focus of law enforcement officers requires providing them with the most complete picture of the known domestic threat posed by terror groups. Information regarding the motives, intentions, and tactics employed by terror groups may help an officer to recognize an otherwise overlooked condition or piece of evidence. For example, a newly emerging trend of domestic and international terror bombers is the use of Triacetonetriperoxide (TATP), which is a highly volatile, highly explosive compound that can be made in the home with commonly available chemicals, including hydrogen peroxide, acetone, and acids. While these compounds are routinely possessed by a majority of Americans, unusual amounts, concentrations, or the fact that all the components are co-located may indicate the intent to mix the chemicals for an unlawful purpose. Without knowledge of TATP and its components, officers could encounter a bomb maker during a routine interaction, see all the components necessary to produce TATP, but fail to recognize the importance of the situation. Armed with timely intelligence, the officer could take immediate action, or forward the information for further investigation.

---

[26] Riley, et al, State and Local Intelligence in the War on Terrorism The Rand Corporation (Santa Monica 2005) 56 Http://www.rand.org/pubs/monographs/2005/RAND_MG394.pdf. Last accessed 01/14/06.

Agencies routinely demand that officers need to report suspicious incidents encountered during their tour. Officers must be continually reminded that reporting information could enable an analyst to combine it with other information, and thereby recognize a larger criminal enterprise. Agencies should retrain officers who are known to keep information proprietary, and commend officers who report pertinent information. To close the communications loop, a process to ensure that relevant terror threat information is delivered back to the officers at the level of operation must also occur.

The concept of intelligence-led policing brings community policing principles and practices into the homeland security effort. Close interactions between police agencies and the community give the police a greater understanding of the events, conditions, and frictions that could signal the possibility of terrorist activity. Patrol officers have constant interactions with the public and are uniquely positioned to serve as direct link between the LE intelligence network and the public. These officers act as the eyes and ears of the intelligence analysts because their duties require them to seek out criminal and suspicious activity in the communities they serve. The true value of this group is their knowledge of local individuals and groups, the races, nationalities and religions represented in the community, and the potential for extremism or terrorism. The officers often develop ability to recognize any abnormal or unusual conditions and behaviors that may develop.[27] And while it may be natural to look for suspicious and illegal activities in areas and groups in which these activities are frequently found racial profiling is to be avoided. Officers walk a fine line between seeking out criminal behavior and the need to treat the vast majority of law-abiding citizens with the respect and trust they deserve. Modern problem solving techniques could be then employed to reduce tension if it appears to be developing within a community.

Community policing partnerships increase the quality and quantity of information moving from community members to the law enforcement. The information can be used

[27] U.S. Department of Justice, Bureau of Justice Assistance *Intelligence-Led policing: The New Intelligence Architecture.* (September 2005) http://www.ojp.usdoj.gov/BJA/pdf/IntelLedPolicing.pdf. Last accessed 11/05/05.

by the intelligence network to identify suspicious or criminal behavior, and the analysis can be used to efficiently allocate resources for the protection of critical infrastructure and other sensitive locations.

One of the challenges that have developed for each law enforcement agency is deciding on the method and frequency of providing threat information to its workforce. Many agencies produce intelligence briefing newsletters designed to quickly, but asynchronously, pass relevant terrorism information to officers working different days, shifts, and locations. Administrators are forced to consider whether it is better to produce a daily intelligence briefing so that the motivated officers have the most current information, balanced with the understanding that producing frequent reports containing virtually no real intelligence related to terrorism (in actuality the document is merely a crime report labeled as a intelligence brief) will eventually lessen the importance of the document, and therefore critical intelligence may be ignored on the rare occasions that it is disseminated. As a result, many agencies have chosen to not produce intelligence briefings on a daily, or weekly basis, but to limit the production of the briefings to those times when viable terror intelligence is developed. This increases the importance of the documents and the relevant information is ultimately more memorable to the recipients. The downside to this is that it is impossible for an analyst to know what local information will resonate with members of the workforce, resulting in the recognition of suspicious behavior.

A primary goal of the intelligence-led policing concept is engaging the community as partners in the homeland security effort; therefore create a local atmosphere inhospitable to any potential terror activity. It is not enough for police to collect and archive information. Rather, unclassified intelligence and relevant threat information can be used to educate the public about security issues, and the kinds of behaviors that should be reported to the police. New York State's Operation Safeguard is an example of how intelligence-led policing techniques can be used as the basis of an anti-terrorism initiative. The New York State Office of Homeland Security (NYSOHS) has enlisted police departments throughout the State to join in this ongoing program intended to identify terrorist planning, surveillance, logistical operations, or any suspicious activity that might be a precursor to a terror event.

A. NEW YORK STATE OPERATION SAFEGUARD

Operation Safeguard operates as a public outreach program designed to generate awareness in the private sectors by providing information regarding potential terrorist indicators and suspicious activities. Participating police agencies enlist local business owners to participate in this anti-terrorism program then conduct regular visits to provide timely threat information. Businesses are provided a certificate of participation, and a poster with instructions to report any suspicious activity to the New York State Toll-Free Tips line. All information generated by the program is recorded by the State, and forwarded to the responsible investigative agency.

When the program was introduced in April of 2004 the NYSOHS had identified seventy categories of businesses and occupations that should be encouraged to participate. Since most local police agencies do not have the resources to handle such a large endeavor, the list of business types that should be actively visited was cut to twelve as of December 2005. The following twelve business types are considered most likely to be exploited by terrorists portraying themselves as legitimate customers seeking to purchase material, licenses, and/or services to covertly further a terror plot are:

- Swimming Pool Supply Stores
- Self Storage Facilities
- Truck/Van/Car Rental Locations
- Real Estate
- Commercial Driving Schools
- Amusement Parks / Mass Gathering
- Agricultural Spraying
- Agricultural and Fertilizer Supply:
- Bulk Fuel
- Chemical Facilities
- Marinas / Boat Rentals and Sales
- Hospitals / Ambulance Service

Since the nature of this program requires regular interactions between the businesses and the local police department, Operation Safeguard helps to establish police / business community relationships where none had existed, and also to strengthen

relationships that do exist. The contacts and interaction facilitate communication on matters relating to terrorism, crime and other matters of mutual concern. The program has an added benefit of directly engaging patrol officers and detectives in a proactive anti-terrorism activity. Performing the business visits reinforces the anti-terrorism commitment of the agency, and ensures that the police officers are kept apprised of recent threat information

In addition to the regular visits, Operation Safeguard can be used to address specific threats. On two occasions in the second half of 2005 the system was utilized to develop information, and to advise merchants about a potential threat.

During October 2005, thousands of Operation Safeguard business locations were contacted based upon a specific, but unconfirmed, intelligence report that terrorists might be planning a chemical attack on the New York City Subway System.[28] Locations such as chemical suppliers, self-storage facilities, and hardware and electrical supply locations were contacted and advised of the active investigation. On November 4, 2005, the NYSOHS released an advisory to police agencies within the state that requested Operation Safeguard contacts be made to radio control aircraft (RCA) clubs and hobby shops. The request, initiated by the Federal Bureau of Investigation, was based upon a concern that an unmanned aerial vehicle (UAV) could be used in a terror attack. The following list of indicators is an abstract of information that was to be discussed with the targeted businesses:

[28] The threat information was released to the public on October 6, 2005. http://www.cnn.com/2005/US/10/06/newyork.subways/. Last accessed 01/12/06.

RCA Clubs should be alert for -

- Requests to utilize facilities or gain access to club property without becoming a member.
- Inquires regarding short-term memberships (i.e. weeks or months).
- Individuals with high-end aircraft, who cannot exhibit rudimentary operational skills.
- Inquiries by individuals who are interested in obtaining operating skills in a very abbreviated time frame.
- Inquiries by individuals who are interested in modifying remote control gliders or model airplanes to enable them to carry a payload, especially installing still or video cameras.

Hobby Shops should be alert for -

- A large cash purchase(s) of remote control gliders or model airplanes by individuals who do not appear to be hobbyists.
- Inquiries by individuals who are interested in modifying remote control gliders or model airplanes to enable them to carry a payload, especially installing still or video cameras.
- A request to purchase gyro systems with digital readouts for remote controlled airplanes. (These are often used by the military in remote drones. These systems allow an airplane to continue on a pre-defined course, even if it loses radio contact with the transmitter.)
- Unusual purchases of chemicals, solvents, propellants, rocket motors, igniters and radio-control equipment associated with various hobbies.
- Unusual inquiries into Kite Aerial Photography, or KAP, which is an obscure hobby that could be used to conduct surveillance on potential targets, without attracting suspicion.

Source: New York State Office of Homeland Security- Advisory Number 375, issued November 04, 2005

The benefits possibly derived from adopting a program similar to Operation Safeguard include:

- Increasing community involvement in the fight against terrorist activity.
- Engaging local police officers in a proactive anti-terrorism effort.
- Strengthening the local community policing relationships.
- Creating a statewide business database.

B. CHAPTER SUMMARY

The effort to reduce the threat and impact of terrorism in the United States requires the creation of a collaborative broad-based network response and law enforcement agencies are in a position to adapt the current intelligence network to provide a platform for this collaboration. The realities of budgeting and finite resources require the identification of strategies that are effective, but scalable so they can be employed regardless of the size of the agency.

Adopting intelligence-led policing techniques will expand a law enforcement agency's ability to reduce crime and improve quality of life issues within their jurisdiction, and will help to identify terrorist activity, and to provide homeland security.

- Administrators should take the time to understand how the intelligence process can be used to achieve the current and future policing goals of the agency. Intelligence and crime analysis should become the basis for developing long-term strategies and future plans.
- Agencies should redouble efforts toward understanding the cultures, beliefs and traditions of the racial, religious and ethnic groups represented in the communities they serve. Special attention should be given to building rapport, establishing mutual trust and creating a commonality of purpose.
- Intelligence should not be hoarded by intelligence analysts or a few select investigators. The national goal of enhancing homeland security will benefit from increasing the ability of all law enforcement personnel to access intelligence.

The patrol force and other law enforcement members who interact with the public should become a conduit for transmitting threat and security information to their individual communities. Patrol officers are in the best position to recognize locations that could be vulnerable to a terror attack, or exploited by terrorist conducting pre-operational activities. Increasing interactions related to homeland security issues will increase the possibility that suspicious actions or conditions are reported.

IV. PUBLIC SECTOR AGENCIES

In order to strengthen the intelligence network's ability to collect, analyze, and disseminate counter-terrorism intelligence, law enforcement agencies must encourage public agencies to become active network participants. Agencies such as Fire, Health, Social Services, Probation, and Public Works all employ members who work within local neighborhoods and have daily interaction with citizens enabling them to become force multipliers for law enforcement. If the public sector workforce is trained to recognize suspicious materials and behaviors, there will be an increased likelihood that pre-operational terrorist activity will be recognized and reported for investigation. Additionally, providing current intelligence regarding the known tactics and suspected targets of terror groups would provide the agencies with the ability to effectively manage resources to harden targets and suggest when new training and defensive strategies may be needed to address changing threats.

Building collaborative and cooperative inter-agency relationships will allow public agencies to support the national anti-terrorism mission. The communication that will result from this intelligence network will allow agencies to share response plans and should reduce friction during critical incidents. Many agencies have critical incident response plans, but few have developed the plans with a full understanding of how their response interacts with agencies from other disciplines. Communication between participants will provide the ability for agencies to develop accurate and coordinated recovery plans. Each agency brings its own unique capabilities and contributions that can be utilized by the intelligence network.

A. PROSECUTORS

As the lead law enforcement agent, prosecutors need to be kept apprised of developing patterns in domestic and international terrorism. As one example, the nature of human interaction has changed rapidly and dramatically since the onset of the cyber age. The internet, cellular telephones, and other means of electronic communication brings a certain anonymity that is being creatively exploited to facilitate criminal

behavior. Terror groups are using these technologies to meet, recruit, and train new members. The groups are also using these same technologies to raise operating funds and coordinate and control group operations.

Including prosecutors in an information sharing network will keep them informed about known terror enterprises and tactics. This will foster mutual understanding and cooperation when the law enforcement agency seeks help for a warrant or attempts to bring charges against suspected terrorists. When necessary, prosecutors can seek legislative help in changing laws or enacting new laws that are needed to address emerging crime trends.

Additionally, since the prosecutor spends a great deal more time with a case than the law enforcement agency did, they will amass a larger amount of knowledge about the suspect and his motives. Most prosecutors also receive criminal cases from many different law enforcement agencies. This gives prosecutors the potential to recognize links or patterns of criminal behavior that may have gone unnoticed by the law enforcement intelligence network.

1. Fire Services

The core function of fire service agencies is in response to active fires. The need for fire response is almost always unexpected and does not allow time for residents to hide evidence of illegal activity. Fire service agencies also gain access to public and private building throughout our local communities when performing regular fire code inspections. This level of access gives Fire Fighters the ability to observe materials that might be used to plan a terror operation, or substances that may be stockpiled for use in an attack.

Many fire service agencies are also trained to respond to incidents involving Hazardous Materials. Since the majority of Haz-Mat incidents involve industrial or transportation accidents with little, or no criminality, keeping Haz-Mat technicians fully informed about known threats and tactics will reduce complacency. The failure to quickly recognize an attack might result in the destruction of key evidence, and the failure to make notifications which would allow other first responders to protect against possible

coordinated attacks. Additionally, failing to recognize an attack will to make fire fighters vulnerable to secondary attacks, or devices which may have been aimed at first responders.

Including the Fire Service agencies in the counter-terrorism intelligence network will increase the number of trained individuals watching for suspicious situations, and will increase the amount of information gathered. Providing the Fire personnel with relevant intelligence may reduce their vulnerability to sustaining injury during a terror attack, and may aid in the preservation of evidence needed for criminal prosecution.

2. Emergency Medical Services

As with the Fire Services, the Emergency Medical Services operate primarily in the response mode. Like the Fire Services, EMS personnel enter homes and private buildings during the normal course of their duties. This access would allow informed medical technicians to recognize suspicious materials or circumstances that might be present in private residences and businesses. Medical technicians also have the ability to investigate the causation of injuries. If a patient is exhibiting signs or symptoms consistent with exposure to hazardous chemicals or substances, the technician could summon the police to investigate, or take note of evidence or testimony, which might be useful in a prosecution.

3. Health Department

The network of Federal, State, and local public health agencies are the primary source of syndromic surveillance and are likely to be the first to detect illness or injury patterns resulting from a biological, chemical, or radiological terror attack. The actions of public health agencies, along with physicians, nurses, and other healthcare providers, are guided by effective protocols for reporting identified illnesses. Additionally, these agencies possess information that would be vitally important to law enforcement agencies, such as plans and procedures to distribute medication in response to mass contaminations, and procedures to expedite the response to mass casualty incidents.

Bioterrorism, pandemic influenza, or infectious diseases are usually viewed as conditions in which law enforcement will have to collaborate with public health, but in

fact the aftermath of any natural or man-made disaster will usually create a aftermath of disease or other health issues that will require public health's involvement.[29] During the rescue and recovery operations at the World Trade Center site in 2001, the NYC Department of Health worked closely with first responder agencies to determine the level of danger that responders and the public faced from the ambient air, and other contaminants.

The Health Department's participation in a counter-terrorism intelligence network will increase the flow of communication between the agencies. Law enforcement agencies can provide the health department with current terrorism intelligence that may facilitate their planning, and may speed in the detection of an attack. This communication system will also allow the health department to keep law enforcement informed regarding the hazards of potential Biological / Chemical attacks. This information will facilitate the development of accurate contingency plans within the law enforcement community.

In addition, the Health Department is the conduit for requesting the deployment of the Strategic National Stockpile of medical supplies. It would be beneficial during a mass casualty incident or weapons of mass effect (WME) emergency if the law enforcement agency had an established and active method of communication with the Health Department.

4. Public Works

The Public Works Department could prove to be a valuable source of information to the intelligence network. Public Works employees are in a unique position to notice trash or refuse that might identify suspicious activity. If the workforce is informed about trends in bomb making, or components of WME's, then they would be more likely to report seeing unusual quantities of these materials. Building Inspectors employed by Public Works regularly inspect public and private buildings, as well as private residences for compliance with local building codes. Providing these individuals with terrorism intelligence would increase their ability to recognize and report suspicious activity.

---

[29] National Governor's Association NGA Center for Best Practices, *Issue Brief, State Strategies for Fully Integrating Public Health into Homeland Security* (Washington D.C. November 2005) from: http://www.nga.org/Files/pdf/FULLYPUBLICHEALTH.pdf. Last accessed 01/19/06.

B. THE LOS ANGELES TERRORISM EARLY WARNING GROUP

Intelligence Fusion center participants have typically been limited to law enforcement, military, and intelligence agencies. The Los Angeles Terrorism Early Warning Group (TEW) is a model of how the resources and expertise of non-law enforcement public agencies can be integrated with those of the law enforcement intelligence network. This collaborative effort provides the ability for coordinated planning and response to acts of terrorism.[30] The TEW was designed to provide a regional coordinated response to terrorism in an area that is home to over 10 million residents, and served by 48 police departments, 38 fire departments, and many other public agencies.

The core participating agencies in the TEW include the Los Angeles County Sheriff's Department, Los Angeles Police Department, Los Angeles Fire Department, Los Angeles County Fire Department, Los Angeles County Health Department, and the Federal Bureau of Investigation. In total, there are approximately thirty Federal, State and local participants, including, law enforcement, fire services, health agencies, emergency management, universities, airports, and transportation. The Los Angeles Sheriff's department acts as the Secretariat providing the facility and handling arrangements for meeting, training sessions, and communications, but the TEW uses the Unified Command structure for direction and decision-making purposes. The ability to access information from any of the participating agencies, combined with the ability to leverage the collective knowledge and experience, provides a unique ability to achieve comprehensive situational understanding.

According to its mission statement, the TEW is charged with "analyzing the Strategic and operational information needed to respond to and combat terrorism and protect critical infrastructure." TEW monitors multi-source information regarding trends and assesses any potential terrorist threat to the Los Angeles region. The assessments produced by TEW analysts are used to guide prevention and mitigation efforts by agencies throughout the region.

---

[30] U.S. Department of Homeland Security, "Terror Early Warning Group" (2005) available on line: http://www.ojp.usdoj.gov/odp/docs/TEWBrochure.pdf#search='Los%20Angeles%20Terrorism%20Early%20Warning%20Group. Last accessed 01/06/06.

In order to facilitate communication between the TEW and its members, each participating agency designates a Terrorism Liaison Officer (TLO) to act as the conduit of information. This TLO system provides a method to ensure that information flows between the agencies and the TEW.

In order to carry out all the functions in the Intelligence Process the TEW is organized into a structure of six cells with separate but interconnected functions.[31]

1. **Officer-in-Charge (OIC/Command):** oversees processes of the TEW, sets intelligence requirements, and is a link to the Unified Command structure.

2. **Analysis/Synthesis:** coordinates analysis and assessment activities – assigning requests for information to the appropriate cells, and developing the results into actionable intelligence products.

3. **Consequence Management:** assesses law enforcement, fire service, and health consequences of events by assessing real-time situation and resource status.

4. **Investigative Liaison:** coordinates with investigation and intelligence teams from Federal, State, and local agencies.

5. **Epidemiological Intelligence:** responsible for real-time disease surveillance, food and water surety, agricultural threat issues, and coordination with the disease investigation.

6. **Forensic Intelligence Support:** provides technical support, chemical, biological, radiological, nuclear and explosive (CBRNE) reconnaissance, geospatial intelligence (mapping, imagery and modeling products), and coordinates "virtual reachback" among the field, TEW and subject matter experts.

[31] U.S. DHS, "Terror Early Warning Group." (4).

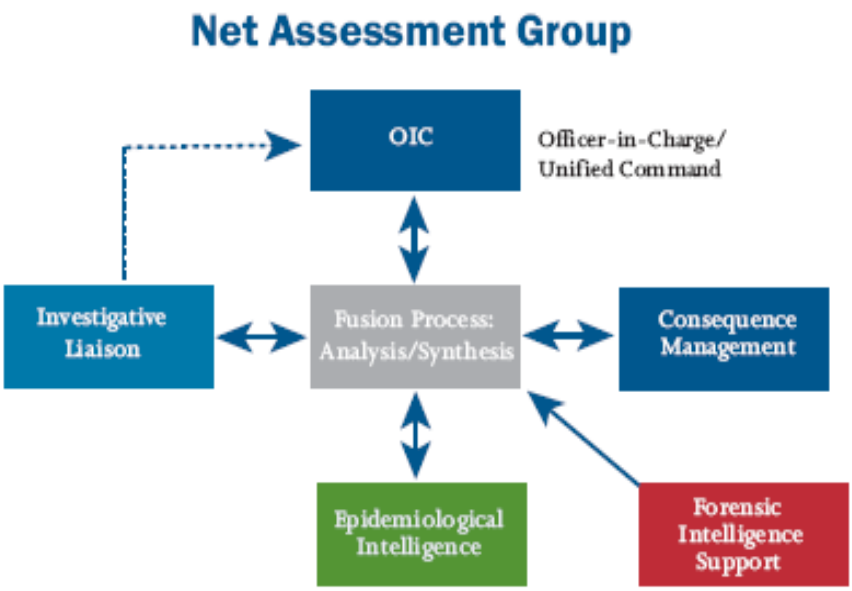

Figure 2. TEW Net Assessment Organization

Relationships between police and public agencies do exist, but prior to 9/11, there was very little incentive for police agencies to share intelligence resources. The paradigm change following the 9/11 attacks has created a desire for information and intelligence on terrorist activities by the public. The paradigm change has also created pressure for these agencies to find new and creative ways to ensure the safety of the public and the national infrastructure. There is an opportunity for both sides to forge a new mindset of cooperation in the effort to enhance homeland security.

Building a new structure of cooperation and coordination will require the increased communication between participants. The establishment of information and intelligence sharing networks between police agencies and other public sector agencies can provide an opportunity to develop systems that will be beneficial in ensuring the public safety. Communication will also help to reduce the cultural differences that currently divide the disciplines. Engaging public sector employees into a counter-terrorism intelligence function and providing them with accurate threat information may also help to reduce unwarranted fears and increase the likelihood that they will continue

to perform vital functions during or after a terror attack. Creating a shared anti-terror mission could act as a form of psychological first aid[32] to limit distress and other adverse health consequences.

The network should provide the ability to transfer terrorist information and intelligence to all the partner agencies based upon their individual needs. *The National Plan for Research and Development in Support of Critical Infrastructure* recommends the development and implementation of systems that "provide an integrated view of societal risks from terrorist events, natural disasters, and other emergencies for incorporation in decision support systems to anticipate and evaluate alternative risk reduction investments and emergency response decisions."[33]

C. WORK GROUPS

Sharing intelligence is not enough. The true basis of an effective local counter-terrorism network is creating a collaborative effort that can be used to further each agency's individual counter-terrorism mission.[34]

Creating a usable product takes commitment and creativity on the part of the Intelligence Analyst. The law enforcement analyst must examine data with an understanding of each partner agency's individual needs. The most functional way to keep the law enforcement analyst aware of these needs is through direct communication and feedback. Regularly scheduled work group meetings will help to build mutual understanding of partner agencies' abilities and limitations. The meetings will also help to coordinate actions between the partner agencies and ensure that the true meaning of the information is understood. Developing a work group will keep local network participants informed about current trends and tactics of terror groups, provide an additional conduit for reporting suspicious activity, and can be used to discuss communications or

---

[32] Adrienne Stith Butler, Allison M. Panzer, Lewis R. Goldfrank, Ed., *Developing Strategies for Minimizing the Psychological Consequences of Terrorism Through Prevention, Intervention, and Health Promotion* (2003, National Academy of Sciences).

[33] Department of Homeland Security. *The National Plan for Research and Development in Support of Critical Infrastructure Protection.* Xi, at: http://www.dhs.gov/interweb/assetlibrary/ST_2004_NCIP_RD_PlanFINALApr05.pdf. Last accessed 11/20/05.

[34] Loyka PERF, 5.

technology issues that may arise. A person-to-person structure of inter-agency communication will greatly enhance the department's ability to interact with network partners. If the law enforcement analysts develop an understanding of how intelligence can be used by partner agencies, they can become attentive to data that may have otherwise gone unnoticed.

Partner agencies should designate a member of their workforce to act as the network point-of-contact, adopting the Terrorism Liaison Officer model used in the TEW. The TLO's should monitor all the interactions associated with their agency's participation, and have a line of communication to their Chief Officer in order to ensure that the exchange of information does not deviate from the agency's mission.

Expanding the law enforcement network to include other public sector agencies is a "force multiplier" in local anti-terrorism efforts. Public agencies can participate by working together in response and recovery planning, and by educating their workforce so that they can recognize and report potential terror activity. Managing the expanded network requires strict monitoring to ensure that essential liberties are not violated in the effort to provide security. This public network must operate with a degree of transparency so that advocacy groups and the media can understand the goals of the program and help the agencies to ensure that they are meeting the public's expectations.

D. DISSEMINATING INTELLIGENCE

> The different forms of intelligence can guide investigations; provide insights for resource allocation; suggest when priorities should be expanded or changed; suggest when new training and procedures may be needed to address changing threats; and permit insight when there is a change in the threat level within a specific community or region.
>
> –David L. Carter
> Guide for State, Local, and Tribal
> Law Enforcement Agencies

In his Guide for State, Local, and Tribal Law Enforcement Agencies, Dr. David L. Carter provides general rules for the release of information. He advocates the

preparation of two versions of an intelligence product if it becomes necessary to release information outside of law enforcement, an unclassified public version, and a "Law Enforcement Sensitive" version.[35] The Law Enforcement Sensitive version would provide more detailed information about suspected terrorists. He makes the claim that "If there is a credible threat to a civilian target it may become necessary that both strategic intelligence and tactical intelligence be disseminated as quickly as possible."[36] Carter defines tactical intelligence as information used to facilitate decision-making during an immediate crisis: the "who, what, when, and where." He defines strategic intelligence as the characteristics, structure and philosophy of the suspected terror group.

Recent improvements in technology allow member agencies to collect, analyze, and disseminate information at a much quicker rate than in the past. The "sensitive but secure" information can be disseminated to partner agencies via fax, email or radio conferencing cell phones. Relevant but less timely information can be shared over web logs administered by the police agency. For example, a web log might post information on missing hospital uniforms. This information is of minor importance unless other participants have found potentially related conditions such as ambulances that are missing license plates, or unqualified persons seeking credentials as emergency responders. Exchanges of this sort would keep the police apprised of suspicious behavior or minor criminal activities that might otherwise go unreported.

1. Ethical Issues of Sharing Intelligence with Public Agencies

The global war on terror is a continuing effort to protect the values to our nation and the safety of our citizens. Law Enforcement's ability to collect information about civilians is regulated and monitored to ensure that civil rights are not violated. If law enforcement agencies are going to exchange information with other public agencies there must be a balance between the need to ensure public safety and the equally important need to preserve civil rights and the public trust.

---

35 David L. Carter PhD, Guide for State, Local, and Tribal Law Enforcement Agencies. (East Lansing: Michigan State University, 2004, 2-4. http://www.cops.usdoj.gov/Default.asp?Item-1404. Last accessed 11/22/05.

36 Carter, *Guide*. 4.

Civil rights organizations will require assurances that public sector information will not be used in domestic spying or illegal information collection. Law enforcement agencies must reassure these groups that any leads coming from public agencies will be investigated to see if there is any potential criminal or terrorist activity. If the investigation rules out criminality, the information will be protected to prevent its use in profiling, denial of services, or infringement of civil liberties. For example, some advocacy groups will certainly be fearful that the program's intent is to use the public sector employees in identifying illegal aliens for deportation. Suspicion of the program could cause emergencies to go unreported or prevent individuals from requesting life sustaining help from the public assistance agencies if individuals fear having their personal information available to the intelligence network.

An effective way to eliminate misconceptions about the purpose of the program is to inform these local groups at the onset about the safeguards utilized to prevent illegal or unethical use of personal information. There needs to be sufficient oversight in place to alleviate fears of privacy infringement and to protect the rights of the local population. The news media could surely play a role in how this program is accepted by the public, but may also be used to further the goals of the program. The best way to prepare for media scrutiny is to limit the program to its intended goals of detecting terrorist activity, and to continuously monitor the program both from the law enforcement end to ensure that rights are not violated, and from the public sector end to ensure that the mechanics of the program do not interfere with the mission of the participating agencies. Providing the media with an overview of the program, and allowing them access to interview employees at the level of operation would help to remove suspicions regarding violation of privacy laws, or actions against the public trust.

The media coverage may also contribute to the success of the program by conveying the impression that the jurisdiction is hyper-vigilant, and a problematic location for terror activity. Public Information Officers should inform the mass media that public agencies are working together to prevent terrorist activity and to develop response and recovery plans.

E. CHAPTER SUMMARY

Combining the resources of local law enforcement agencies with the resources of the public and private sector is an important step in developing a network response to homeland security issues and the protection of vital infrastructure. The system of exchanging information / intelligence between partner agencies could be incorporated as part of an agency's intelligence-led policing strategy. Even smaller law enforcement agencies with limited resources can become a communications conduit between local public agencies and a State or regional law enforcement intelligence system.

- Law enforcement agencies should institute regular electronic communications with public agencies to create a coordinated and cooperative local effort to fight terrorism and enhance homeland security.
- All partner agencies should designate a member of their workforce to act as the network point-of-contact, adopting the Terrorism Liaison Officer model used in the TEW. This contact person should monitor all the interactions associated with their network participation, and have a line of communication to their agency's Chief Officer in order to ensure that the exchange of information does not negatively affect their agency's mission.
- In addition to the electronic communication, each law enforcement agency should conduct regularly scheduled working group meetings to build mutual understanding of each partner agency's strengths, limitations and their ability to contribute to the effort. The working group meetings should also be used to coordinate preparedness issues and planning.
- Law enforcement agencies should create two forms of the intelligence product. One version should be “law enforcement sensitive” and contain the information needed for law enforcement purposes. The other version should be “Public Sector Sensitive” and contain information that would be useful to public agencies.
- All sharing of information between law enforcement and other public agencies should be limited to that which is allowed by law, and should not violate civil rights, or the public trust.
- Law enforcement agencies should conduct regular reviews of intelligence cases to determine if the goals of the expanded network are being attained and essential liberties are being protected.
- Dissemination Review- All information that will be released from the Intelligence Unit to the public agency partners should be rechecked to ensure that it will not endanger any active investigations or sources.

V. PRIVATE SECTOR AGENCIES

> More than anything else, homeland security in the 21st century is about the integration of an entire nation, as well as, depending on the circumstances, the integration of nations themselves. It's a philosophy of shared responsibility, shared leadership and shared accountability. And the private sector has a critically important role to play in this all-hands effort. We need partners in the private sector that will stand up and be counted as any regular citizen, partners that take an active forward-leaning view of security at all times.
>
> *– Secretary of Homeland Security Tom Ridge, Cargo Security Summit, Washington, DC, 16 December 2004.*

A. THE POST-9/11 PARADIGM SHIFT FOR LAW ENFORCEMENT, AND THE NEED FOR CHANGE

In light of the additional burdens that have been recognized in the five years since the 9/11 terrorist attacks, we should acknowledge that law enforcement agencies do not have the capacity to provide complete security coverage within their jurisdictions. Law enforcement agencies usually have patrol assets, and they have the ability to access terrorist threat information, but most do not have the capacity to provide real security at the infinite number of potential terrorist targets. The vast majority of these potential targets are owned and protected by private sector entities.

In order to enhance local law enforcement's ability to attain the strategic goals outlined in the National Strategy for Homeland Security,[37] it is essential to incorporate the resources that are available in the private sector. According to the Gilmore Commission's Second Report, approximately 85% of the nation's workforce and infrastructure is controlled by the private sector.[38] Based upon a suspected threat, members of law enforcement agencies have the authority to consult with, and even assist the private sector in increasing security at privately controlled locations. Police agencies have the legal authority in criminal matters, but generally have little understanding of the

[37] The *National Strategy for Homeland Security*.

[38] U.S. Congress. The Gilmore Commission Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. Santa Monica: the RAND Corporation, 2002.

broad range of private security functions, expertise, and resources, and often fail to appreciate the role of private security.[39] It is more than likely that the persons who have the daily responsibility for protecting the location will have a better understanding of the possible vulnerabilities, the ramifications of a successful attack, and the best way to increase security to protect against an attack.

Regardless of the anti-terrorism and counter-terrorism efforts undertaken at either the public or the private level, the possibility of a successful attack cannot be discounted. Based on that understanding, most private sector security providers make provisions to ensure the continuity of their business operations after natural or man-made disasters. Many companies have built redundancies into their daily operations, secondary information technology sites, cooperative agreements with similar agencies, and other contingency planning to recover or replace affected assets so they can resume normal operations as soon as possible. Ironically, the intelligence that the private sector could surely use to defend against, or quickly recover from an attack is the same intelligence that law enforcement is often unable or unwilling to share.

Utilizing the vast resources available in the private sector requires the development of a new structure of coordination and cooperation between local law enforcement agencies and private companies. A recent study conducted in cooperation with the International Association of Chiefs of Police (IACP) by the Justice Department's Community Oriented Policing Services (COPS) corroborates this claim. According to *Private Security/Public Policing Partnerships* in 2000 there were 17,784 state and local law enforcement agencies in the United States, employing 708,000 full-time sworn officers. In addition, there were 88,500 federal law enforcement officers, bringing the public total to about 797,000 public law enforcement officers.[40] By contrast, recent studies of private security suggest there may be as many as 90,000 private security organizations employing roughly 2 million security officers in the United States.[41] The study suggested, however, that only five to ten percent of law enforcement chief

[39] U.S. Congress. The Gilmore Commission.

[40] IACP, COPS. 2004. Private Security/Public Policing Partnerships. 2 http://www.cops.usdoj.gov/mime/open.pdf?Item=1355. Last accessed 12/08/05.

[41] Ibid. 2.

executives participate in any collaborative partnerships with private security. Similarly, emergency response exercises tend to include police, fire, public health, and other governmental authorities but exclude agencies responsible for private security. The study recommends that leaders of the major law enforcement and private security organizations should endorse the implementation of sustainable public–private partnerships in order to address terrorism, public disorder, and crime. The paper advocates several ways to bridge the gap, such as communication networks, joint training seminars, and the establishment of public/private professional organizations.[42]

In an article published in Foreign Policy Magazine, David Rothkopf also advocates private industry's participation in the war on terror. He says, "…private-sector players can deploy innovative technologies and unlimited financing to fort U.S. cities, battle cyber threats, track the movements of terrorists, and disarm biological weapons."[43] In spite of the benefits, Rothkopf believes the majority of federal, state, and local agencies have yet to take advantage of the resources offered by private sector organizations. He claims that "to date, these companies have been involved in very little of the coordinated planning, drilling exercises, threat evaluation, intelligence sharing, cooperative research, or any of the other steps a national defense strategy requires."[44]

If a "secure but sensitive" information network is to succeed, the potential benefits of participation will surely have to outweigh the costs. For the law enforcement agency, the benefit will be increased security at critical infrastructure sites, as well as enhanced ability to collect information about terrorism and other criminal activity from private sector participants. The cost for the law enforcement agency will be the investment in resources such as manpower, IT equipment, and office space. Many local law enforcement agencies currently maintain an Intelligence Unit that would provide the expertise in disseminating information.

Private companies, by necessity, make most decisions based upon economic factors; with regard to terrorism, there are other incentives for cooperation. The prospect of losing company assets and or employees to a terror event should provide the necessary

[42] IACP, COPS, 3.

[43] David J. Rothkopf, "Business versus Terror." *Foreign Policy130* (May/June 2002): 56.

[44] IACP/COPS, 57.

incentives for private sector decision- makers to make the relatively low-cost investment in network participation. The companies could assign manpower to receive the terrorist information, and then transmit it to any employee who deals with security concerns. The company would also communicate any suspicious behavior or other relevant information back to the law enforcement agency. As Dr. Ruth David explains, "The need for timely sharing of information… is well documented--but unfulfilled." She points out the need for information to be shared with the private corporations who "own and operate much of the nation's infrastructure--and may be directly targeted for attack."[45]

Since there is a paucity of viable terrorist information available to local police agencies, the network needs to transmit other information of mutual interest in order to maintain the program. Transmitting reports of crimes that just occurred, with descriptions of offenders, will allow the police agency to increase the number of eyes looking for a fleeing suspect. This enhancement of crime-fighting resources becomes a value-added benefit to police agencies looking to close cases. The value-added benefit for the private agency is the quick access to information they would otherwise not have. The police agency could transmit information about road closures to network participants, who could then re-route their fleets around congested traffic. Information transmitted on crime patterns, or crimes that just occurred, would allow private agencies to take temporary or precautionary measures. For example, if a banking concern received alerts about a subject who just robbed two banks in the area, they could prepare dye packs, or alert the police if the subject tried to enter one of their bank locations.

1. Ethical Issues of Sharing Intelligence with Private Agencies

Just as with public agencies, the exchange of information between law enforcement and private agencies must be balanced between the need to ensure public safety and the equally important need to preserve civil rights and to public trust. Law enforcement agencies must ensure that any sharing of information between law enforcement and private agencies is limited to that which is allowed by law, and does not violate civil rights, or target any ethnic, racial or religious group. Transparency and

[45] Ruth David, "Homeland Security Technologies: Creating an Asymmetric Advantage." *Journal of Homeland Security*, 2002: 24.

openness with the news media and with civil rights groups regarding the goals and practices of program will help to alleviate misunderstanding. Publicity of the public / private partnership will also contribute to increasing public awareness of homeland security issues, and build public confidence.

B. THE SECURITY POLICE INFORMATION NETWORK

Although many officials in the field of homeland security are calling for the creation of information sharing partnerships, there are very few active, successful programs. The Nassau County Police Department's Security Police Information Network (SPIN) is an example of an effective, active information-sharing network. Few information networks of this nature are currently providing timely dissemination of information from the federal government to state and local law enforcement agencies and onto private infrastructure and security officials. SPIN was designed to be a crime prevention partnership between the Nassau County Police Department (NCPD) and the private sector that seeks to increase public safety through the sharing of important and timely information. The program was started in August 2004 in order to incorporate the resources of the private sector into Nassau County's effort to fight terrorist activity.

As outlined in Chapter III, community policing strategies call upon law enforcement agencies to develop relationships with various sectors of the community. Police departments meet regularly with local clergy, business groups, neighborhood associations, and other groups. Prior to 9/11, there was little contact with corporate security directors or managers of security businesses.[46] Since the establishment of SPIN, NCPD administrators have been in contact with business groups and associations to encourage participation. As of December 2005, the NCPD has vetted over 900 individual participants into the program, and is actively recruiting additional members. The vetting process is comprised of local background and criminal history checks performed by the department's Applicant Investigation Unit. The vetting process has so far shown that most applicants have a great deal of training, and have New York State certifications in security- and law enforcement-related fields. Many of the applicants are former federal, state, or local law enforcement officers.

[46] IACP and COPS, Private Security/Public Policing Partnerships, 24.

The stated goals of SPIN are to share information, identify and discuss crime trends and solutions, work together toward the common goal of protection of persons and assets, and create a better working relationship between law enforcement and the private sector.[47] SPIN members are contacted by email or text messaging and informed of unfolding situations as they occur. Messages include terror threat information, bank robberies (and attempts), major road closures, disruptions in public transportation, major fires or explosions, suspicious packages or circumstances, civil disturbance, public health or weather-related emergencies, or any other situations involving public safety or affecting continuity of business. Members of the group are able to exchange information about planned evacuation drills or other safety matters. In addition, monthly meetings are held to discuss timely security-related issues.

The establishment of such a comprehensive network has far-reaching applications. From assisting in the capture of felony suspects or notification of the latest crime trends, to helping business to do business through traffic delay notifications, SPIN can facilitate the large-scale exchange of information. The Network also provides the ability to distribute training materials that may enhance the safety of everyone who lives or works in Nassau County.[48]

SPIN enables the police department to send out information tailored to specific sectors of private industry. Each sector (colleges and universities, hospitals, grade schools, malls and retail businesses, utility companies, petroleum companies, technology companies, hotels and motels, financial institutions, and corporate security) is sorted into its own email distribution sub-group as well as a general distribution group. The sub-group members receive sector-specific information. An unspecified threat against electrical power plants would go only to the utilities group; threats to schools go only to the education group, and so on. These categories mirror the ones utilized by the Homeland Security Information Network (HSIN) operated by the Department of Homeland Security.[49] HSIN provides a Critical Infrastructure Morning Briefing

[47] Nassau County Police Department Deputy Inspector Matthew Simeone, interview by author, Mineola, NY, 5 January 2005.

[48] Ibid.

[49] Homeland Security Information Network, at http://www.dhs.gov/dhspublic/interapp/press_release/press_release_0354.xml. Last accessed 03/02/06.

newsletter, which is disseminated over SPIN. The newsletter provides open-source intelligence separated into the listed categories. In addition, SPIN messages are sent to all law enforcement agencies operating in Nassau County, as well as Metropolitan Transportation Authority police, and other federal, state or local agencies in adjoining counties.[50]

A continuous challenge is deciding how to disseminate intelligence to the various law enforcement and security partners. NCPD analysts create two versions of relevant counter terrorism intelligence, a "Law Enforcement Sensitive" version and a "Sensitive but Secure" version that omits any classified or restricted material. The "sensitive but secure" information is disseminated to SPIN network participants via fax or email. The NCPD is considering the implementation of industry-specific web logs to transmit relevant but less timely information. For example, a web log set up for utility companies might post information about damaged locks found at un-manned facilities. This information is of minor importance unless other companies have found similar conditions at their facilities. Exchanges of this sort would keep the police apprised of potentially important activities that might otherwise go unreported.

In order for this network to succeed in enhancing counter terrorism strategies, agency partners must understand the need to act on the intelligence, promptly transmit the information throughout their workforce, and to report any relevant incidents or circumstances back to the Intelligence Unit.

Administration of a public/private communications network has associated costs, such as physical facilities, IT equipment, staffing, and training issues. Department officials have considered charging private security agencies to participate in the network, but have not instituted such a fee because of indications that the fee might cause smaller companies to drop out of the program. To date, the NCPD has absorbed all costs into its operating budget. The allocation of resources for public/private partnerships is analogous to allocating resources for emergency and crisis management. The real benefits of any such investments may not be recognized or appreciated until an actual crisis arises.

[50] Nassau County is policed by one county police agency, and 21 smaller city and village police departments.

C. CHAPTER SUMMARY

Law enforcement agencies do not have the capacity to provide real security at the infinite number of potential terrorist targets. The vast majority of these potential targets are owned and protected by private sector entities. In order to increase the flow of information to the law enforcement intelligence network, and build a cooperative local homeland security effort, law enforcement agencies must include private sector security companies in their local communications network.

- Law enforcement agencies should institute regular electronic communications with private sector security providers to improve the local effort to fight terrorism and enhance homeland security. The system utilized to communicate with public sector agencies can be used to send information to private sector partners.
- All private agency partners should designate a member of their workforce to act as the network point-of-contact. This contact person should monitor all the interactions associated with their network participation, and have a line of communication to their agency's Chief Officer in order to ensure that important information is transmitted, and necessary actions are taken.
- In addition to the electronic communication, each law enforcement agency should conduct regularly scheduled working group meetings to build mutual understanding of each private partner agency's informational needs and their ability to contribute to the homeland security effort.
- Law enforcement agencies should create an additional “Sensitive but Secure” version of the intelligence product. This version should contain the information needed for private sector partners to recognize pre-operational activity, and enhance security at sensitive sites.
- All sharing of information between law enforcement and private agencies should be limited to that which is allowed by law, and should not violate civil rights, or the public trust.

VI. RECOMMENDATIONS

The effort to reduce the threat and impact of terrorism in the United States requires the creation of a collaborative broad-based network response. Law enforcement agencies are in a position to adapt the current intelligence network to provide a platform for this collaboration. The realities of budgeting and finite resources require the identification of strategies that are effective, but scalable so they can be employed regardless of the size of the agency.

Every law enforcement agency, even smaller agencies that lack a staff dedicated to providing intelligence analysis, can still perform all the functions of the intelligence process. The National Incident Management System has been adopted as the national model for critical incident management. Since NIMS protocol dictates that the incident command structure must include the ability to gather, share and manage incident-related intelligence, the existing law enforcement intelligence architecture should be used to provide this function.

- Law enforcement administrators should develop a better understanding of the mechanics of the intelligence process within their agency and recognize the benefits of using intelligence in developing short and long term crime reduction strategies, homeland security planning, and incident management requirements.

In order to fully participate in a national effort against terrorism each law enforcement agency needs a direct line of communication with a comprehensive national source of terrorist intelligence. The National Counter-Terrorism Center is the primary organization within the U.S. Government for the analysis and integration of foreign and domestic intelligence related to terrorism. Law enforcement agencies receive unclassified intelligence developed at the National Counter-Terrorism Center through intermediary agencies such as the FBI and DHS.

- Local agencies should press for legislation that empowers the NCTC to create a single direct path for the flow of actionable and relevant intelligence to State and local law enforcement agencies.
- Local agencies should also ask for legislation that creates a State and Local Intelligence Council under the Director of National Intelligence for the purpose of improving national intelligence to support State, local, and tribal efforts.

In an effort to facilitate the flow of intelligence, the FBI has instituted a program to provide Secret security clearances to decision makers in local law enforcement agencies.

- Local agencies should designate members to apply for the Secret classification and thereby access information that could be used to enhance local security plans and direct enforcement efforts.

Since there is no single-source national intelligence link, the law enforcement intelligence network participants are required to access information and intelligence using data sources such as RISS, ATIX, LEO, and JRIES. These electronic sources provide the ability to push local and proprietary data and intelligence up to the regional and national level enabling the recognition of patterns and trends that exist beyond the local level.

- Local agencies must push Federal officials to develop a primary electronic intelligence network that can link the Federal, State and local law enforcement partners. A single intelligence link with help to eliminate the gaps that exist between the NCTC and local agencies.
- Local agencies must push Federal officials to provide a national intelligence education system that allows law enforcement intelligence analysts to understand basic standards and adopt best practices.

The co-location of multi-agency intelligence resources in a Fusion Center enables analysts to call upon the information and collection abilities of all participating agencies and then integrate that data to produce a more complete intelligence product. Although many agencies lack the resources to assign resources to a Fusion Center, the participating Federal and State agencies usually disseminate the resulting intelligence products to all local agencies.

- Local law enforcement agencies must appeal to State officials to ensure that fusion centers are structured to support both national intelligence and local intelligence led policing needs.

A. INTELLIGENCE-LED POLICING TECHNIQUES

The effort to reduce the threat and impact of terrorism in the United States requires the creation of a collaborative broad-based network response and law enforcement agencies are in a position to adapt the current intelligence network to provide a platform for this collaboration. Adopting intelligence-led policing techniques will expand a law enforcement agency's ability to reduce crime and improve quality of

life issues within their jurisdiction, and will help to identify terrorist activity, and to provide homeland security. The patrol force and other law enforcement members who interact with the public should become a conduit for transmitting threat and security information to their individual communities. Patrol officers are in the best position to recognize locations that could be vulnerable to a terror attack or exploited by terrorist conducting pre-operational activities. Increasing interactions related to homeland security issues will increase the possibility that suspicious actions or conditions will be reported.

- Agencies should redouble efforts toward understanding the cultures, beliefs and traditions of the racial, religious and ethnic groups represented in the communities they serve. Special attention should be given to building rapport, establishing mutual trust and creating a commonality of purpose.
- Agency administrators must insure that intelligence is not hoarded by intelligence analysts or a few select investigators. The national goal of enhancing homeland security will benefit from increasing the ability of all law enforcement personnel to access intelligence.

1. Public Sector Agencies

Combining the resources of local law enforcement agencies with the resources of the public sector is an important step in developing a network response to homeland security issues and the protection of vital infrastructure. The system of exchanging information / intelligence between partner agencies could be incorporated as part of an agencies intelligence-led policing strategy. Even smaller law enforcement agencies with limited resources can become a communications conduit between local public agencies and a State or regional law enforcement intelligence system.

- Law enforcement agencies should institute regular electronic communications with public agencies to create a coordinated and cooperative local effort to fight terrorism and enhance homeland security.

Expanding the law enforcement network to include other public sector agencies is a “force multiplier” in local anti-terrorism efforts. Public agencies can participate by working together in response and recovery planning, and by educating their workforce so that they can recognize and report potential terror activity. Law enforcement agencies should create two forms of the intelligence product. One version should be “law enforcement sensitive” and contain the information needed for law enforcement

purposes. The other version should be “Public Sector Sensitive” and contain information that would be useful to public agencies. In addition to the electronic communication, each law enforcement agency should conduct regularly scheduled working group meetings to build mutual understanding of each partner agency's strengths, limitations and their ability to contribute to the effort. The working group meetings should also be used to coordinate preparedness issues and planning.

Managing the expanded network requires strict monitoring to ensure that essential liberties are not violated in the effort to provide security. This public network must operate with a degree of transparency so that advocacy groups and the media can understand the goals of the program and help the agencies to ensure that they are meeting the public’s expectations. All sharing of information between law enforcement and other public agencies should be limited to that which is allowed by law, and should not violate civil rights, or the public trust.

All public partner agencies should be encouraged to designate a member of their workforce to act as the network point-of-contact. This contact person should monitor all the interactions associated with their network participation, and have a line of communication to their agency's Chief Officer in order to ensure that the exchange of information does not negatively affect their agency's mission.

Once this public sector communications network is developed law enforcement agencies should conduct regular reviews of intelligence cases to determine if the goals of the expanded network are being attained and essential liberties are being protected. All information that will be released from the Intelligence Unit to the public agency partners should also be rechecked to ensure that it will not endanger any active investigations or sources.

2. Private Sector Agencies

Law enforcement agencies do not have the capacity to provide real security at the vast number of potential terrorist targets. The large majority of these potential targets are owned and protected by private sector entities. In order to increase the flow of information to the law enforcement intelligence network, and build a cooperative local

homeland security effort, law enforcement agencies must include private sector security companies in their local communications network.

- Law enforcement agencies should institute regular electronic communications with private sector security providers to improve the local effort to fight terrorism and enhance homeland security. The same system utilized to communicate with public sector agencies can be used to send information to private sector partners.

All private agency partners should designate a member of their workforce to act as the network point-of-contact. This contact person should monitor all the interactions associated with their network participation, and have a line of communication to their agency's Chief Officer in order to ensure that important information is transmitted, and necessary actions are taken.

In addition to the electronic communication, each law enforcement agency should conduct regularly scheduled working group meetings to build mutual understanding of each private partner agency's informational needs and their ability to contribute to the homeland security effort.

Law enforcement agencies should create an additional “Sensitive but Secure” version of the intelligence product. This version should contain the information needed for private sector partners to recognize pre-operational activity, and enhance security at sensitive sites.

All sharing of information between law enforcement and private agencies should be limited to that which is allowed by law, and should not violate civil rights, or the public trust.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Baird, Zoë, and James Barksdale. "There is Security in Sharing." *San Jose Mercury News,* August 16, 2004.

Berman, Jerry, and James X. Dempsey. *Information Sharing and Civil Liberties.* Center for Democracy and Technology. Article. (last accessed 12/05/05 from http://www.cdt.org/security/20041004informationsharing.pdf

Butler, Adrienne Stith; Allison M.Panzer; and Lewis R Goldfrank, Ed. Developing Strategies for Minimizing the Psychological Consequences of Terrorism Through Prevention, Intervention, and Health Promotion. 2003, National Academy of Sciences.

Carter, David L. PhD. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*. (East Lansing, Michigan State University, 2004) (http://www.cops.usdoj.gov/Default.asp?Item=1404) (last accessed 11/22/05).

David, Ruth, PhD. Homeland Security Technologies: Creating an Asymmetric Advantage. Journal of Homeland Security (April 2002).

Department of Homeland Security. *The National Plan for Research and Development in Support of Critical Infrastructure Protection.* http://www.ojp.usdoj.gov/odp/docs/TEWBrochure.pdf#search='Los%20Angeles%20Terrorism%20Early%20Warning%20Group' (last accessed 01/06/06)

———. *Intelligence-Led Policing: The New Intelligence Architecture* Washington D.C., 2005.

———. Office of Justice Programs. *National Criminal Intelligence Sharing Plan.* Washington D.C., 2003.

Department of Justice. *Law Enforcement Analytic Standards.* Washington D.C., 2004. U.S. http://it.ojp.gov/documents/law_enforcement_analytic_standards.pdf (last accessed 05/10/05)

———. "The FBI's Counterterrorism Program Since September 2001" 14 April 2004. 65. Available online: http://www.fbi.gov/publications/commission/9-11commissionrep.pdf (last accessed 12/15/05).

Federal Emergency Management Agency, *The National Incident Management System.* http://www.nimsonline.com/ics_org_charts/intel_2.htm Downloaded 09/15/05.

The Gilmore Commission Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. The Rand Corporation, December 2000.

International Association of Chiefs of Police. Private Security/Public Policing Partnerships. 2004.(http://www.cops.usdoj.gov/mime/open.pdf?Item=1355). (last accessed 12/08/05.

Johnson, Loch K., and James J Wirtz. *Strategic Intelligence: Windows into a Secret World.* Los Angeles: Roxbury, 2004.

Kean, Thomas H., and Lee H Hamilton. *The 9/11 Commission report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* New York: W.W. Norton, 2004.

Lowenthal, Mark M. *Intelligence from Secrets to Policy*. Washington D.C.: CQ Press, 2003.

National Governor's Association. NGA Center for Best Practices, *Issue Brief, State Strategies for Fully Integrating Public Health into Homeland Security*, Washington D.C., November 2005.

——NGA Center for Best Practices. *Issue Brief*: *Establishing State Intelligence Fusion Centers.* National Governor's Association Washington D.C., July 2005.

Loyka et al. *Protecting the Community from Terrorism, volume 4*. Washington D.C. Police Executive Research Forum, 2005) (http://policeforum.mn-8.net/default.asp?link=%2Fdocs%2Fdocapp%2Easpx%3F%5Fcommand%3Ddetail%26%5Fappid%3D5%26id%3D41645%26%5FclientInfo%3D%253cclientInfo%253e%253cfid%253e%2D1%253c%252ffid%253e%253c%252fclientInfo%253e) (last accessed 09/21/05).

O'Hanlon, Michael E. "Homeland Security: How Police Can Intervene." *The Washington Times*, August 18, 2004.

Office of Homeland Security. *National Strategy for Homeland Security*. Washington D.C. 2002 (http://www.whitehouse.gov/homeland/book/nat_strat_hls.pdf) (last accessed 05/20/05.

Riley, et al. State and Local Intelligence in the War on Terrorism The Rand Corporation Santa Monica. 2005. Http://www.rand.org/pubs/monographs/2005/RAND_MG394.pdf (last accessed 01/14/06

Rothkopf, David J. *Business versus Terror*. Foreign Policy. May/June 2002. Issue 130

Steinberg, James B. *Consolidating Intelligence Analysis: A Review of the President's Proposal to Create a Terrorist Threat Integration Center*. Report before the Senate Governmental Affairs Committee, February 14, 2003. Last accessed 11/22/05 from: (http://www.brook.edu/views/testimony/steinberg20030214.htm)

Treverton, Gregory F. The Next Step in Reshaping Intelligence. RAND Corporation. Santa Monica. 2005.

THIS PAGE LEFT INTENTIONALLY BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California